



Highlights of [GAO-06-527T](#), a testimony to the House Committee on Government Reform

Why GAO Did This Study

For many years, GAO has reported that ineffective information security is a widespread problem that has potentially devastating consequences. In its reports to Congress since 1997, GAO has identified information security as a governmentwide high-risk issue—most recently in January 2005.

Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, Congress passed the Federal Information Security Management Act of 2002 (FISMA), which permanently authorized and strengthened the federal information security program, evaluation, and reporting requirements established for federal agencies.

This testimony discusses:

- The federal government’s progress and challenges in implementing FISMA, as reported by the Office of Management and Budget (OMB), the agencies, and the Inspectors General (IGs).
- Actions needed to improve FISMA reporting and address underlying information security weaknesses.

www.gao.gov/cgi-bin/getrpt?GAO-06-527T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshusen@gao.gov.

INFORMATION SECURITY

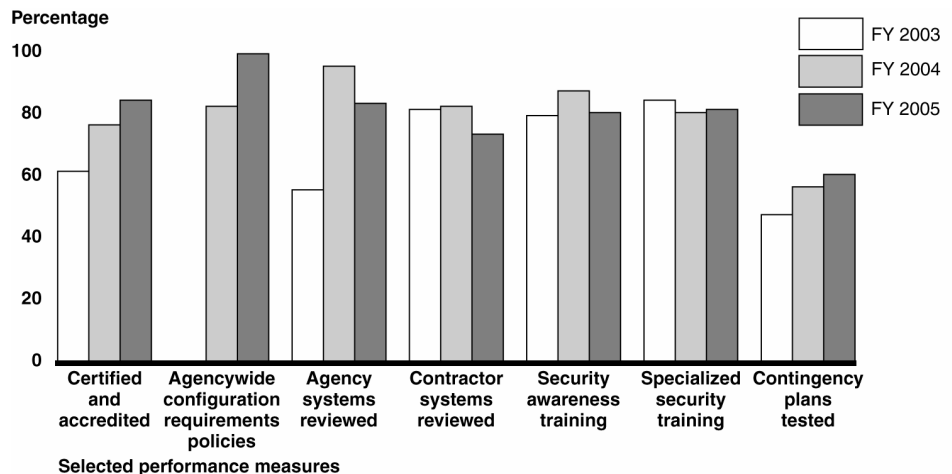
Federal Agencies Show Mixed Progress in Implementing Statutory Requirements

What GAO Found

In its fiscal year 2005 report to Congress, OMB discusses progress in implementing key information security requirements, but at the same time cites challenging weaknesses that remain. The report notes several governmentwide findings, such as the varying effectiveness of agencies’ security remediation processes and the inconsistent quality of agencies’ certification and accreditation (the process of authorizing operation of a system, including the development and implementation of risk assessments and security controls). Nevertheless, fiscal year 2005 data reported by 24 major agencies, compared with data reported for the previous 2 fiscal years (see fig.), show that these agencies have made steady progress in certifying and accrediting systems, although they reported mixed progress in meeting other key statutory information security requirements. For example, agencies reported that only 61 percent of their systems had tested contingency plans, thereby reducing assurance that agencies will be able to recover from the disruption of those systems with untested plans.

Federal entities can act to improve the usefulness of the annual FISMA reporting process and to mitigate underlying information security weaknesses. OMB has taken several actions to improve FISMA reporting—such as requiring agencies to provide performance information based on the relative importance or risk of the systems—and can further enhance the reliability and quality of reported information. Agencies also can take actions to fully implement their FISMA-mandated programs and address the weaknesses in their information security controls. Such actions include completing and maintaining accurate inventories of major systems, prioritizing information security efforts based on system risk levels, and strengthening controls that are to prevent, limit, and detect access to the agencies’ information and information systems.

Reported Data for Selected Performance Measures for 24 Major Agencies



Source: GAO analysis of agencies’ FY2003-2005 FISMA reports.